Department of Justice
U.S. Attorney's Office
Eastern District of North Carolina

FOR IMMEDIATE RELEASE Wednesday, January 22, 2020

Venezuelan Man Sentenced for Aggravated Identity Theft and Access Device Fraud

RALEIGH – United States Attorney Robert J. Higdon, Jr. announced that United States District Judge James C. Dever III sentenced **RICARDO ABDEL,** of Doral, Florida, to 48 months imprisonment, followed by 3 years of supervised release and ordered them to pay $19,966.71 in restitution. **ABDEL,** a permanent resident alien from Venzuela, was named in a two-count Criminal Information charging Access Device Fraud and Aggravated Identity Theft. **ABDEL** pled guilty to those charges on March 20, 2019.

In March 2018, the Wilmington Police Department (WPD) was alerted by investigators with the State Employees' Credit Union (SECU) fraud division of ongoing fraudulent debit/credit card withdrawals being made from member accounts at various automated teller machines (ATMs) in the Wilmington area. On March 5, 2018, the United States Secret Service (USSS) was notified by the SECU and the WPD that three individuals were attempting to illegally withdraw money from an SECU ATM located on Wrightsville Avenue in Wilmington. Officers responded to that location and conducted a traffic stop of a vehicle in which **ABDEL** and two other persons were riding. A search of the vehicle revealed approximately $9,319 in United States currency, numerous debit/credit cards, computers, digital storage media, and two debit/credit card readers/encoders.

Investigators with the SECU's fraud unit and the USSS determined that the fraudulent debit/credit cards were used at multiple ATM locations in the Wilmington area over a period of several days. Further, the SECU's fraud unit confirmed that an illegal debit/credit card skimming device had been placed on a SECU ATM in Leland, North Carolina. A forensic search of the seized laptop computers and cell phones revealed 566 individual card numbers which were issued by 71 different financial institutions, including 7 card numbers which were issued by financial institution in Mexico and 1 from India. The intended loss was calculated at $283,000.

On July 3, 2018, investigators received credible information identifying co-conspirators based in Venezuela and in the Miami, Florida, area who were involved in the scheme to commit access device fraud. The conspirators downloaded credit card data from Bluetooth debit/credit card skimming devices which were secretly installed in Tritan ATMs. After obtaining the debit/credit card and personal identification numbers (PIN) from the debit/credit card skimming devices, the coconspirators used a credit card reader/writer to reencode counterfeit debit/credit cards. In March 2018, **ABDEL** and his conspirators used the fraudulent debit/credit cards at ATMs in the Wilmington area to withdraw funds from multiple victims' accounts. The investigation revealed that the group was traveling to various states, including Georgia, California, and Florida, to

install debit/credit card skimming devices. It is estimated that the group made $250,000 monthly as a result of the fraudulent scheme.

Additionally, investigators learned that in March 2018, **ABDEL** spent four or five days in the Wilmington area placing pin-hole camera skimming devices on ATMs and collecting account numbers. Those numbers were then encoded onto magnetic stripe cards and used to fraudulently withdraw funds from ATMs. **ABDEL** and the others also travelled to the Wilmington area two to three weeks earlier in order to recover debit/credit card skimming devices and computers which were left in a suitcase in a storage unit by another coconspirator.

The United States Secret Service, the Wilmington Police Department and the Kure Beach Police Department conducted the investigation. Assistant United States Attorney Ethan Ontjes represented the government.